

WHAT IS CLAIMED IS:

1. A method for identifying digital object using digital watermark, comprising:
 - (a) encrypting a message derived from source data on the digital object to obtain an encrypted message digest (S); and
 - (b) deriving a watermark from the encrypted message digest (S) and incorporating into the source data.
2. A method according to claim 1 wherein the message is obtained via performing a hash function on the source data on the digital object to obtain a message digest (M) on the digital object, and wherein the message digest (M) is the message encrypted with the signature encryption key to obtain the encrypted message digest (S).
3. A method according to claim 1 wherein the watermark is a physical domain watermark and the method further comprises incorporating the physical domain watermark to at least a portion of the source data.
4. A method according to claim 3 further comprising transforming a frequency domain vector (U) derived from the encrypted message digest (S) to physical domain in deriving the watermark.

5. A method according to claim 4 further comprising deriving the frequency domain vector (U) by modulating at least a portion of the encrypted message digest (S) to obtain at least a portion of the vector (U).

6. A method according to claim 5 wherein a portion of the vector (U) corresponds to low frequencies and another portion of (U) corresponds to high frequencies, the portion of U corresponding to low frequencies being derived by modulating at least a portion of the encrypted message digest (S).

7. A method according to claim 6 wherein the portion of the vector (U) corresponding to low frequencies are modulated to have more significant impact on amplitude of the watermark than the portion of the vector (U) corresponding to high frequencies.

8. A method according to claim 7 wherein the portion of the vector (U) corresponding to low frequency has negative value in elements corresponding to "0" bits of the at least a portion of the encrypted message digest (S) and has positive value in elements corresponding to "1" bits of the at least a portion of the encrypted message digest (S); and wherein the portion of (U) corresponding to high frequencies have elements of zero value.

9. A method according to claim 1 wherein the source data consist of rows and columns of pixels and the watermark is represented by a watermark vector (W)

having a dimension corresponding to the number of rows (m) or the number of columns (n) of the pixels.

10. A method according to claim 9 wherein a pixel contains data on a discrete section of an image object.

11. A method according to claim 9 wherein a pixel contains data on a discrete section of audio object.

12. A method according to claim 9 wherein the watermark incorporated into the source data is orthogonal to the data to which the watermark is added.

13. A method according to claim 9 further comprising deriving from the source data a source data vector (A) having the same dimension as that of the watermark vector (W) by selecting at least a portion of the source data and further comprising deriving the watermark vector (W) based on the encrypted message digest (S) such that watermark vector (W) is orthogonal to source data vector (A); and further comprising combining the watermark vector (W) with the data in the selected portion of the source data from which source data vector (A) is derived to form watermarked data.

14. A method according to claim 9 further comprising comparing the at least a portion of the source data before incorporation of the watermark to after incorporation of the watermark.

15. A method according to claim 14 further comprising finding the correlation between the watermark vector (W) and a target vector (X) derived from data suspected of containing the watermark, wherein said target vector (X) is orthogonal to the source data to which the watermark is incorporated.

16. A method for identifying data using digital watermark, comprising:

(a) performing a one-way function on source data to obtain a message digest (M);

(b) encrypting the message digest (M) with a signature encryption key to obtain an encrypted message digest (S);

(c) deriving a frequency domain vector (U) from the encrypted message digest (S) by modulating a portion of the encrypted message digest (S) corresponding to low frequencies more than a portion corresponding to high frequencies;

(d) transforming the frequency domain vector (U) into a physical domain key vector (V);

(e) selecting a portion of the source data and deriving a watermarking vector (W) from the frequency domain vector (U) orthogonal to the selected source data; and

(f) combining the selected source data with the watermarking vector (W) in the physical domain.

17. A system for identifying data using digital watermark, comprising:

(a) means for encrypting a message derived from source data with a signature encryption key to obtain an encrypted message digest (S); and

(b) means for deriving a watermark from the encrypted message digest (S) and incorporating into the source data.

18. A system according to claim 17 further comprising a means for performing a hash function on the source data to obtain a message digest (M) and wherein the means for encrypting encrypts the message digest (M) with the signature encryption key to obtain the encrypted message digest (S).

19. A system according to claim 17 wherein the water mark is a physical domain watermark and the means for deriving incorporates the physical domain watermark to at least a portion of the source data.

20. A system according to claim 19 wherein the means for deriving derives a frequency domain vector (U) from the encrypted message digest (S) and transforms the vector (U) to physical domain in deriving the watermark.

21. A system according to claim 20 wherein the means for deriving derives the frequency domain vector (U) by modulating at least a portion of the encrypted message digest (S) to obtain at least a portion of the vector (U).

22. A system according to claim 21 wherein the means for deriving manages the source data as rows and columns of pixels and derives a watermark vector (W) based on the vector (U), the watermark vector (W) having a dimension corresponding to the number of rows (m) or the number of columns (n) of the pixels.

23. A system according to claim 22 wherein the means for deriving derives from the source data a source data vector (A) having the same dimension as that of the watermark vector (W) by selecting at least a portion of the source data and wherein the watermark vector (W) is orthogonal to source data vector (A).

24. A system according to claim 23 further comprising a means for comparing a set of target data with the source data, the means for comparing compares a target vector (X) derived from the target data to the source data, the target vector (X) being orthogonal to the source data vector (A).

25. An article of manufacture comprising a program storage medium, tangibly embodying a program code means readable by a computer to cause the computer to identifying a digital object using a digital watermark, comprising:

- (a) code means for performing a one-way function on source data on the digital object to obtain a message digest (M) on the source data;
- (b) code means for encrypting the message digest (M) with a signature encryption key to obtain an encrypted message digest (S);

(c) code means for deriving a watermark from the encrypted message digest (S) via a transforming a portion of the message digest (S) as frequency domain into a physical domain before resulting in a one-dimensional watermark for incorporating into the source data; and

(d) code means for incorporating the one dimensional watermark into the source data.